FIG.1

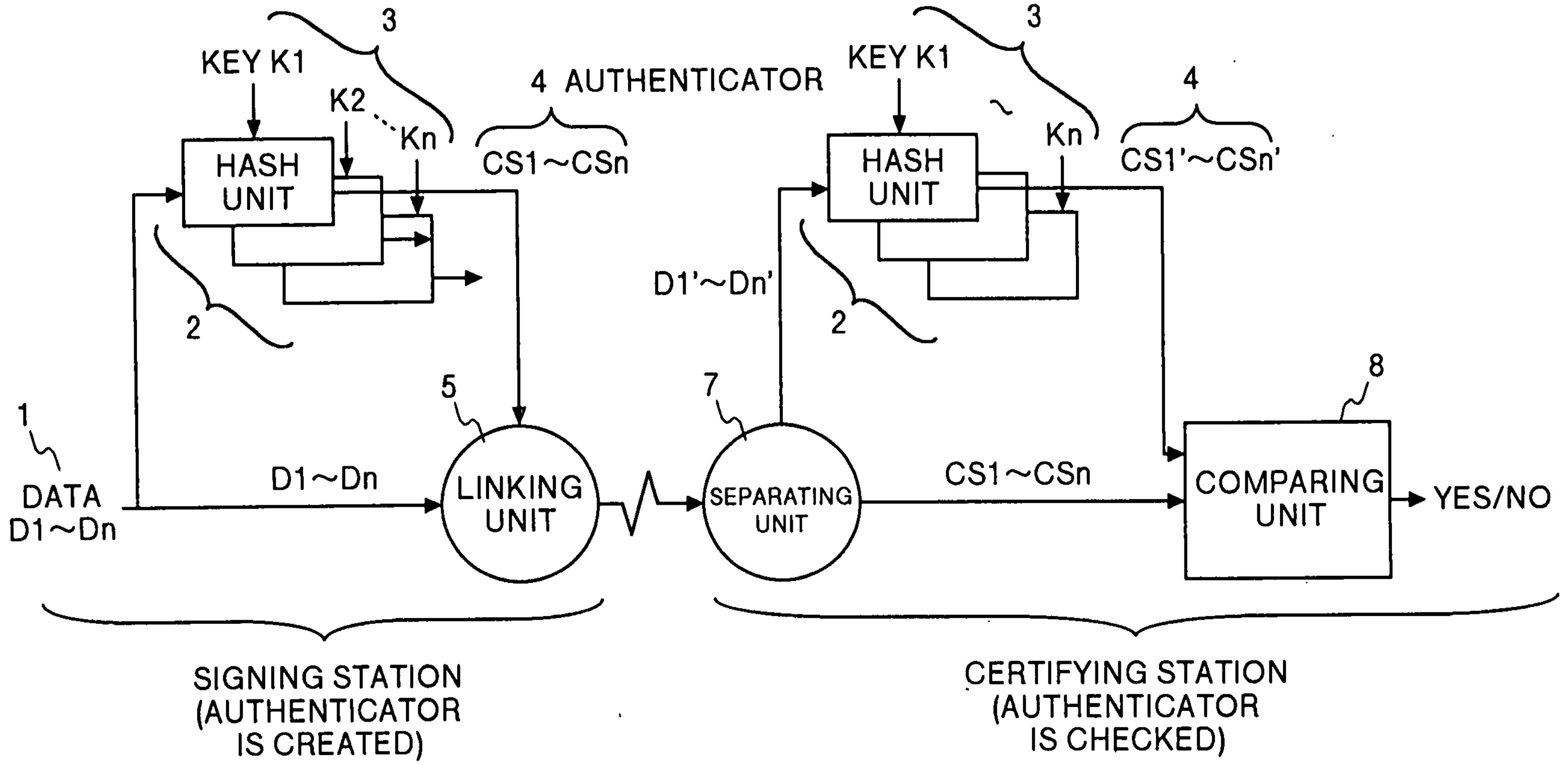

KEY K1
3
K2
Kn
HASH UNIT
2
4 AUTHENTICATOR
CS1~CSn
1
DATA D1~Dn
D1~Dn
5
LINKING UNIT
SIGNING STATION (AUTHENTICATOR IS CREATED)
KEY K1
3
Kn
HASH UNIT
2
D1'~Dn'
4
CS1'~CSn'
7
SEPARATING UNIT
CS1~CSn
8
COMPARING UNIT
YES/NO
CERTIFYING STATION (AUTHENTICATOR IS CHECKED)

FIG.2A

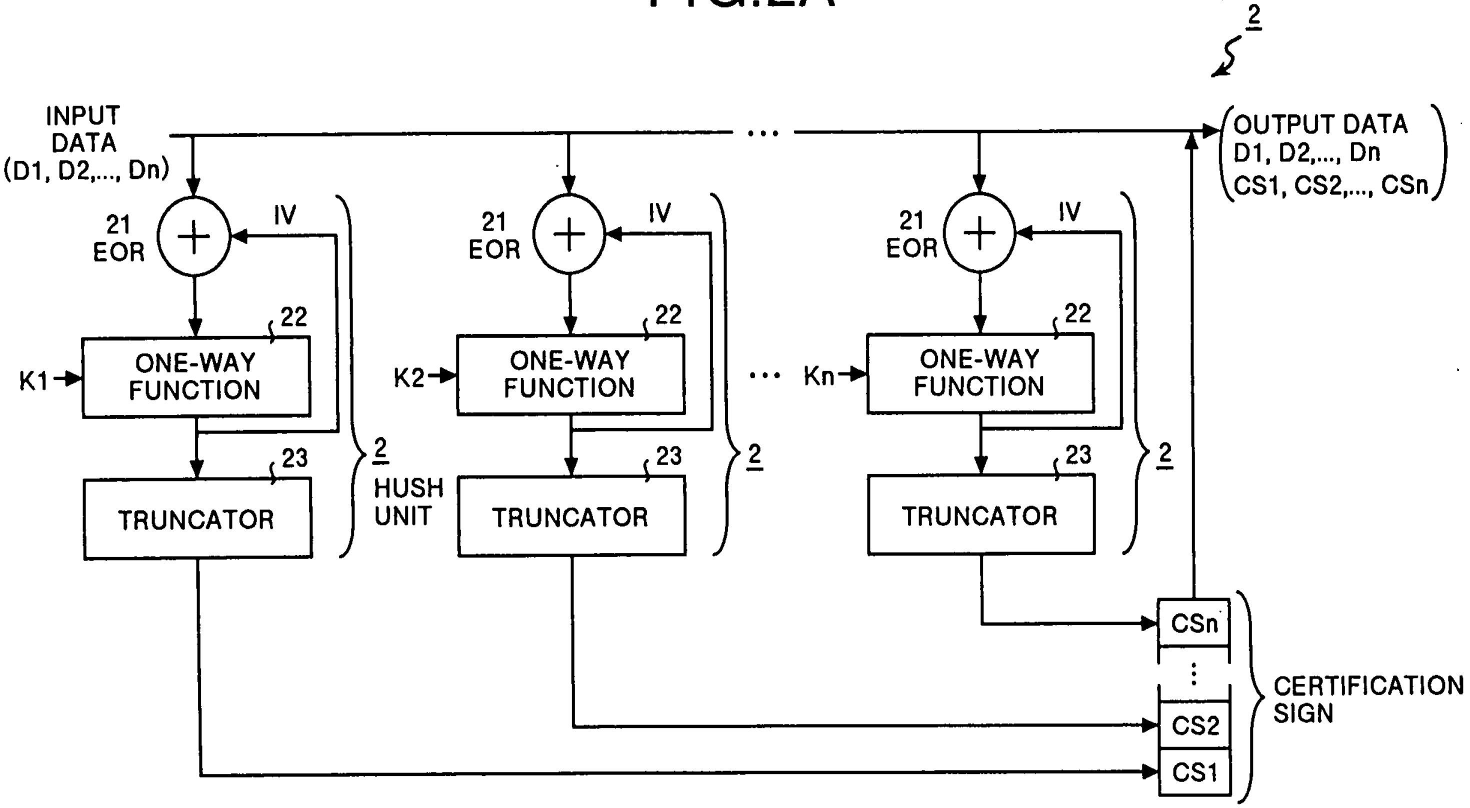


FIG.2B

(b-1)CS1-GENERATING PROCESS
①→IV=PUBLIC CONSTANT
②→EK1[IV(+)D1]=L11
③→EK1[L11(+)D2]=L12
• • • • •
④→EK1[L1(n-1)(+)Dn]=L1n
⑤→Tr[L1n]=CS1

(b-2)CS2-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
• • • • •
EK2[L2(n-1)(+)Dn]=L2n
Tr[L2n]=CS2

(b-3)CS3-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
• • • • •
EK3[L3(n-1)(+)Dn]=L3n
Tr[L3n]=CS3

FIG.3A

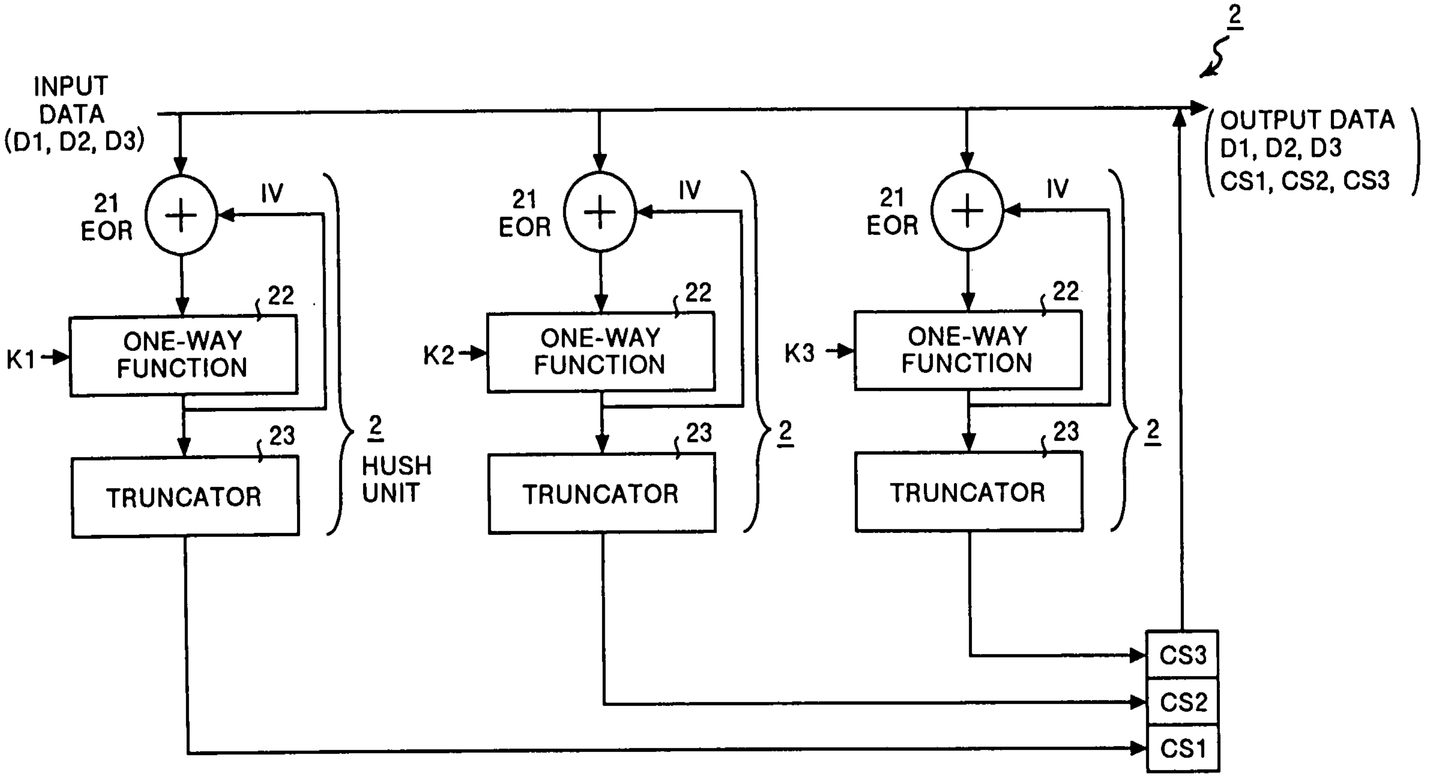


FIG.3B

(b-1)CS1-GENERATING PROCESS
①'→IV=PUBLIC CONSTANT
②'→EK1[IV(+)D1]=L11
③'→EK1[L11(+)D2]=L12
④'→EK1[L12(+)D3]=L13
⑤'→Tr[L13]=CS1

(b-2)CS2-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
EK2[L22(+)D3]=L23
Tr[L23]=CS2

(b-3)CS3-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
EK3[L32(+)D3]=L33
Tr[L33]=CS3

FIG.4A

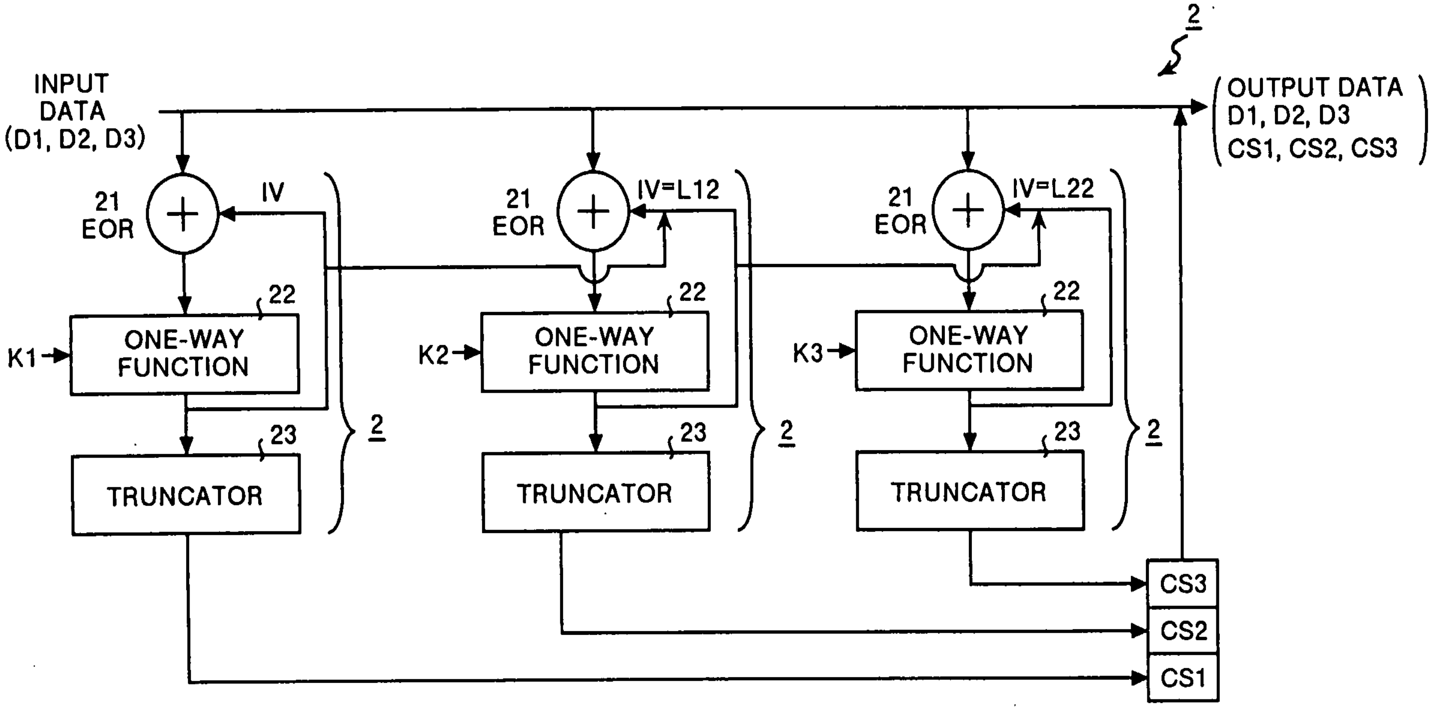


FIG.4B

(b-1)CS1-GENERATING PROCESS

IV=PUBLIC CONSTANT
EK1[IV(+)D1]=L11
EK1[L11(+)D2]=L12

EK1[L12(+)D3]=L13

Tr[L13]=CS1

⑥

(b-2)CS2-GENERATING PROCESS

IV=L12
EK2[IV'(+)D1]=L21
EK2[L21(+)D2]=L22

EK2[L22(+)D3]=L23

Tr[L23]=CS2

⑦

(b-3)CS3-GENERATING PROCESS

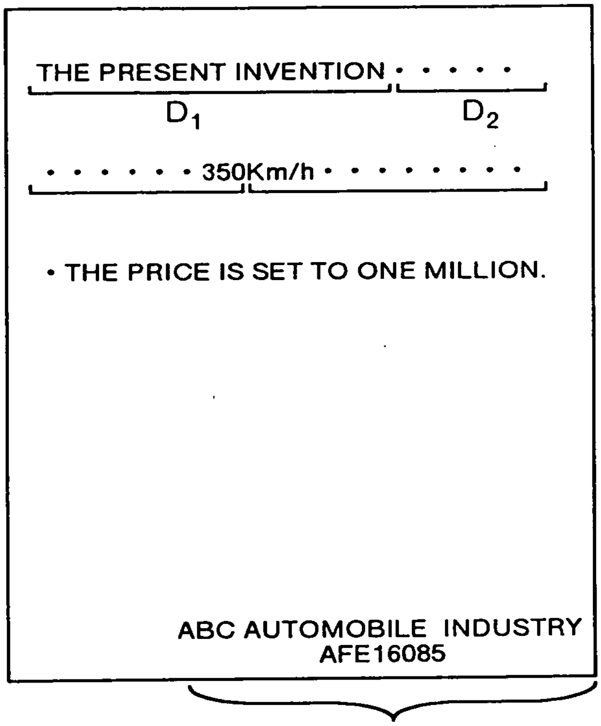
IV=L22
EK3[IV"(+)D1]=L31
EK3[L31(+)D2]=L32

EK3[L32(+)D3]=L33

Tr[L33]=CS3

FIG.5

EXAMPLE OF A DOCUMENT



THE PRESENT INVENTION • • • • •
D1
D2
• • • • • • • 350Km/h • • • • • • • • •
• THE PRICE IS SET TO ONE MILLION.
ABC AUTOMOBILE INDUSTRY
AFE16085

EXAMPLE OF A AUTHENTICATOR IN A DES-MAC SYSTEM
8 DIGITS (1 DIGIT=4 BITS)

FIG.6A

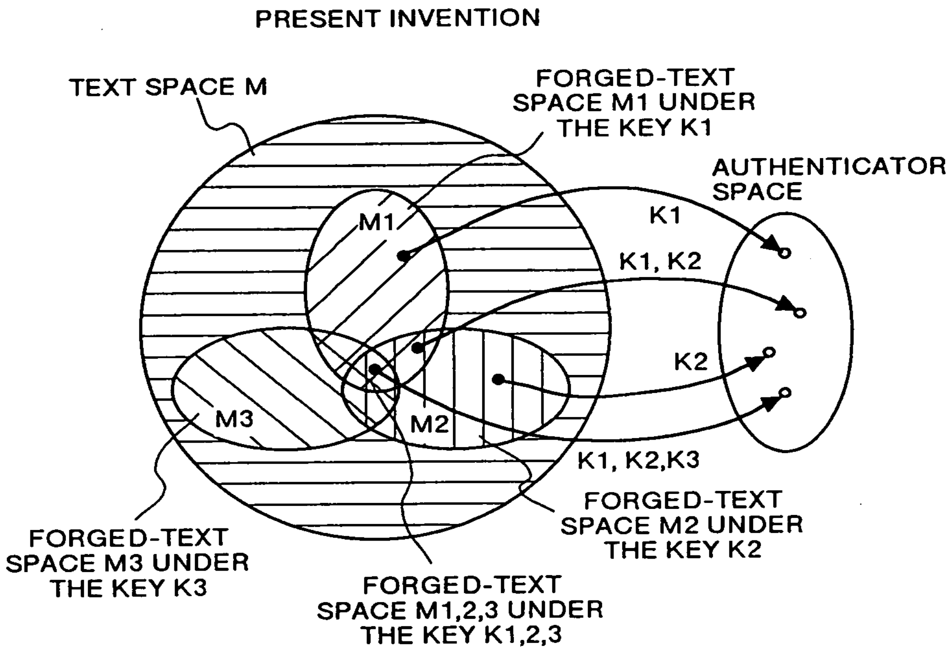
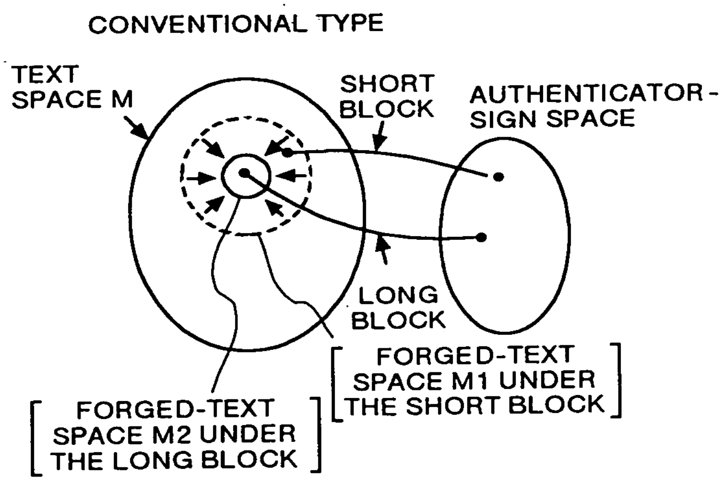

PRESENT INVENTION
TEXT SPACE M
FORGED-TEXT SPACE M1 UNDER THE KEY K1
AUTHENTICATOR SPACE
M1
K1
K1, K2
K2
M3
M2
K1, K2,K3
FORGED-TEXT SPACE M2 UNDER THE KEY K2
FORGED-TEXT SPACE M3 UNDER THE KEY K3
FORGED-TEXT SPACE M1,2,3 UNDER THE KEY K1,2,3

FIG.6B


CONVENTIONAL TYPE
TEXT SPACE M
SHORT BLOCK
AUTHENTICATOR-SIGN SPACE
LONG BLOCK
FORGED-TEXT SPACE M1 UNDER THE SHORT BLOCK
FORGED-TEXT SPACE M2 UNDER THE LONG BLOCK